REMARKS

Claims 27-38 are pending. Claims 1, 3-5, 8-13, 15, 18, 19, and 23-26 were rejected and have been canceled, without prejudice. Claims 27-38 are new. Reconsideration and allowance are respectfully requested.

Summary of Examiner Interview

Applicants thank examiner Melvin H. Pollack for spending time to discuss the outstanding office action with applicants' attorney Marc E. Brown and inventor Professor Joseph Touch over the telephone on June 12, 2009.

A predecessor version of new claim 27 was discussed. (New claim 27 is identical to the claim which was discussed, except that it makes clear that "tether" and "anchor" are coined terms unique to the invention, not terms of art.) Following some discussion, the examiner agreed that new claim 27 appeared to be patentable over the applied references. Applicants agreed to file a Request for Continued Examination and to document key distinguishing points in these remarks.

Problem With Earlier Technology

Computers on the Internet require addresses, much like telephones require phone numbers. These addresses fall into two categories: public and private. Public addresses are also called publicly routable addresses because they can be reached (routed to) from other public addresses. Private addresses are also called unroutable because they cannot be reached from other public addresses -- these addresses do not appear in the routing tables of routers on the public Internet.

Public addresses can be used as both the source and destination of a connection. Computers with public addresses can initiate connections to other computers (e.g., contact Google with a request to look up). They can also receive connections, so other computers can call them (e.g., host a web server, Internet telephone, or peer-to-peer file sharing software). Due to the limited number of public addresses, it has become common to configure a device called a Network Address Translator (NAT) with a single public address on its public side, allowing multiple computers to use private addresses hidden behind that device. The NAT translates the addresses (and sometimes other header parameters) of packets between its public and private sides. NATs are commonly integrated into home DSL routers and cable modems.

NATs allow computers from its private side to contact computers on its public side, but not the converse.[1] Private-side computers can 'call out', but they cannot receive incoming calls, because the translation table is configured by the first outgoing (private to public) packet. This limitation can be an impediment to many modern capabilities, e.g., running a local web server to monitor computer configurations (e.g., as Toshiba does for software upgrades), running independent local web servers (e.g., to host various web pages in general), running Internet telephony services, or running peer-to-peer services. Many such systems can require cumbersome mechanisms that handshake through other computers elsewhere on the Internet, rather than "direct dialing" each other as do computers on the public Internet (see U.S. PGPub 2006/0215684 and its included prior art discussion).

A similar effect with protected and unprotected addresses results from the use of a firewall that similarly impairs communication between these groups of addresses.

Invention of New Claim 27

New claim 27 is a method for communicating with a plurality of devices behind the private side of a NAT, each through a different publicly routable network address.[2] A request is issued from a client behind the private side of the NAT to a server on the

[1] A NAT can be configured to send all incoming connections to a single device, or to allow connections with a-priori known parameters to contact particular private devices. However, they cannot generally allow private devices to run independent copies of the same service; i.e., it is not usually possible to run multiple web servers on the private side of the NAT so that they are accessible from the public side.

[2] Support for this new claim may be found in the pre-grant publication of this application at, for example, paragraphs [0029], [0033], [0034], [0036], [0038], [0040], [0041], [0044], [0046], [0062], [0063]. Should the examiner nevertheless have a question, the examiner is invited to phone applicants' attorney Marc E. Brown at 310-788-1569.

public side of the NAT for the publicly routable network addresses. The request is delivered from the client to the server through the NAT. The publicly routable network addresses is received at the client from the server through NAT.

A router behind the private side of the NAT – which applicants have descriptively named herein a tether router -- is configured to associate each of the devices behind the private side of the NAT with at least one of the publicly routable network addresses. A tunnel is configured through the NAT between the tether router and a router on the public side of the NAT – which applicants have descriptively named herein an anchor router. Packets can be exchanged between the tether router and the anchor router through the NAT without being translated by the NAT.

Packets addressed to at least one of the publicly routable network addresses are received at the tether router from the anchor router encapsulated within the tunnel through the NAT. The received packets are forwarded from the tether router to the device that has been associated within the tether router to the at least one publicly routable network address to which the packets are addressed.

This unique method can provide a wide variety of equally unique services. Home Internet users can run their own public services, such as web servers and peer-to-peer servers, on any number of home computers without requiring permission from or coordination with their ISP. Home Internet users can access files on any of multiple home PCs or storage servers, e.g., personal video recorders (PVRs, e.g., TIVOs) from any remote location. Users can deploy services and otherwise enjoy unfettered Internet access on any number of local devices, at trade shows and remote meetings at hotels, coffee shops, and other commercial establishments typically offering restricted Internet service. Purveyors of rented equipment, such as copiers and postage machines, can monitor their machines remotely even when those machines are deployed inside protected corporate environments. The net effect is that communications to the plurality of devices behind the private side of the NAT are effectuated using publicly routable network address.

Deficiencies in Applied References

In the last office action, Cheline et al. (7,197,550) and Carrico et al (2003/0135616) were primarily relied upon. However, whether alone or in combination, they do not permit communications with devices behind the private side of a NAT to be effectuated using publicly routable network addresses, as required by new claim 27.

Cheline configures a VPN and connects it via a modem 106 to a VPN concentrator 136 through a VPN tunnel to a local network 156. As part of this configuration, Cheline configures firewall 134 and/or NAT function 228 implemented in memory 210 in modem 106. However, Cheline does not disclose a method to traverse either a NAT or a firewall so as to allow communications to a plurality of devices behind the private side of a NAT using publicly routable network addresses – the fundamental function of this new claim.

Carrico does not make up for this fundamental deficiency. Carrico describes a tunnel between either two hosts (two IPsec clients) or between a host (an IPsec client) and a router (IPsec gateway). Carrico does not disclose a tunnel between two routers, such as between what applicants have descriptively termed a tether router and an anchor router, as required by new claim 27.

Carrico also only provides secure tunneling access for a single private IP address – that of the IPsec client on the private side of the NAT (in either of the cases described). It does not support tunneling for a plurality of publicly routable network addresses, as also required by new claim 27.

It would also not be obvious to modify Cheline to use these features of Carrico. Cheline teaches to cooperate with and utilize NATs, while Carrico teaches to avoid their affects. It would not be obvious to combine a method for configuring a NAT with a method of avoiding a NAT (by traversing it). The two approaches are contradictory – Cheline supports the use NATs, whereas Carrico supports avoiding the effect of a NAT. Indeed, it is not even apparent how their respective functions could be combined into a single harmonious system.

The combination of Cheline and Carrico would also still be far from the invention of new claim 27. Even combined, for example, packets would not be received at a tether router from an anchor router encapsulated within a tunnel that traverses a NAT addressed to at least one of the publicly routable network addresses which is associated with one of the devices within the tether router.

These references are also incapable of providing the unique benefits which the invention of new claim 27 can provide. For example, whether alone or in combination, these references do not explain how to configure a network of devices on the private side of a NAT so that each can be individually accessed from public addresses, without having to configure the hosts on the public side of the NAT and the NAT itself.

New Claims 28-38

New claim 31 is the same as new claim 27, but recites a firewall as the device which blocks packet traversals in either direction based on packet header or content.[3] Also, "private" and "public" in new claim 27 has replaced, respectively, with "protected" and "unprotected" in new claim 31 to be consistent with terminology that is commonly used to describe firewalls.

New claims 35 and 37 are system counterparts to new claims 27 and 31, respectively.[4]

The remaining new claims are all dependent new claims 27, 31, 35, and 37, and thus are patentable in view of the applied references for the same reasons.[5]

[3] Support for this new claim may be found in the paragraphs cited above in footnote 1 for new claim 27. Again, should the examiner nevertheless have a question, the examiner is invited to phone applicants' attorney Marc E. Brown at 310-788-1569.

[4] They are replacements for the system claims which were previously presented.

[5] The elements added by these new claims are essentially the same as were recited in now-canceled claims 4, 5, and 12. Again, should the examiner nevertheless have a question, the examiner is invited to phone applicants' attorney Marc E. Brown at 310-788-1569.

CONCLUSION

For the foregoing reasons, Applicant respectfully submits that the above amendment places this application in condition for allowance, which Applicant respectfully solicits.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 501946 and please credit any excess fees to such deposit account and reference attorney docket no. 28080-107.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Marc E. Brown
Registration No. 28,590

2049 Century Park East, 38th Floor
Los Angeles, CA 90067
Phone: (310) 277-4110
Facsimile: (310) 277-4730
Date: June 18, 2009

Please recognize our Customer No. 33401 as our correspondence address.